

Notice of Allowability

Application No.

09/931,291

Examiner

Eleni A. Shiferaw

Applicant(s)

KAASHOEK ET AL.

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 03/23/2007.
2. ☒ The allowed claim(s) is/are 1,3-9,11-19,21,22 and 24-27.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

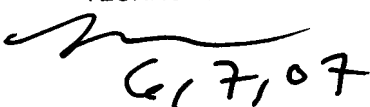
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 6/1/07.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


6,7,07

DETAILED ACTION

1. A telephone interview was made, to request a formal terminal disclaimer for double patenting rejection made in the previous office action, and to request an approval for examiner's amendment on the claims that raised 112, 101 issues and examiner's amendments to particularly point out the invention, with Denis G. Maloney.

Based on the interview, the applicant filed a terminal disclaimer to disclaim the terminal portion of the term of the entire patent of current application to the expiration date of "USPN 7,043,759" and the office on 6/6/07 has approved the terminal disclaimer.

The examiner's amendment has been made as follows for claims 1, 9, 18, 21, and 22 based on the telephone interview.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Denis G. Maloney on June 1, 2007

3. Claims 1, 9, 18, 21, and 22 are amended as follows.

1. (Currently Amended) A control system, comprising:

a computer system to coordinate thwarting attacks on a data center that is coupled to a network ~~the~~ the computer system comprising:

a communication device, coupled to a physically separate network from the network that the data center is coupled to, to receive statistical data collected from network traffic flows collected by a plurality of monitors dispersed through the network that the data center is coupled to, with the monitors sending the statistical data collected from the network that the data center is coupled to over the physically separate network from the network that the plurality of monitors collect the statistical data from;

with the computer system executing:

a process to analyze the statistical data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic;

a process to identify gateways on the monitoring network that are sources of malicious traffic destined for the data center; and

a filtering process to eliminate the malicious traffic from entering the data center.

9. (Currently Amended) A method, executed on a computer system, the method comprises:

receiving by the computer system statistical data from a plurality of monitors, dispersed through ~~the~~ a network, with the monitors sending the statistical data collected from the network

over a second, different network, that is a physically separate network from the network that the plurality of monitors collect data from;

analyzing in the computer system the statistical data from the plurality of monitors to determine network traffic statistics that can identify sources of malicious network traffic; and

determining in the computer system a filtering process to install on devices in the network that the monitors collect data from to inhibit the malicious network traffic from entering ~~the~~ a victim data center[[.]] ; and

installing the filtering process on the devices to inhibit the malicious network traffic from entering the victim data center.

18. (Currently Amended) A computer program product stored in a computer storage to coordinate ~~thwarting attacks~~ an attack on a data center that is coupled to a network, the computer program product comprises instructions to cause a computer to:

receive data from a plurality of monitors, dispersed through a first network that is coupled to the ~~victim~~ data center, with the monitors sending statistical data collected by the monitors from the first network over a second, different network, that is a physically separate network from the first network that the plurality of monitors collect data from;

analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic;

determine a filtering process to install on at least one device in the network that the monitors collect data from to inhibit the malicious traffic from entering the data center; and

coordinate measures to locate and block ~~the~~ a sources of ~~an~~ the attack.

21. (Currently Amended) A control center system, comprising:

a computer system, configured as the control center to coordinate thwarting of attacks on a data center that is coupled to a first network, the control center executing:

a communication process that executes on the computer system to receive statistical data from and send messages to a plurality of monitors dispersed through the network, with the communication ~~device and~~ process sending the messages and receiving the statistical data from the monitors over a second, different network, that is a physically separate network from the first network that the plurality of monitors collect data from;

and

an analysis process that executes on the computer system to analyze the statistical data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic and to send the messages to the monitors to control monitors in the network to coordinate thwarting an attack on the ~~victim~~ data center; and

a process to aggregate traffic statistics from the plurality of monitors to use in coordinating measures to locate and block ~~the~~ a sources of ~~an~~ the attack.

22. (Currently Amended) The system of claim 21 further comprising:

a process that executed on the computer system to select a filtering process to eliminate the malicious traffic from entering the victim data center.

Response to Arguments

2. Applicant's amendments and arguments filed on 02/13/2007 are persuasive.

Allowable Subject Matter

3. The following is an examiner's statement of reasons for allowance: a search of the prior art fails to teach or render as obvious the claims feature as a whole and of particular note:

Wherein a control center system/method/program to coordinate thwarting attacks on a data center that is coupled to a network comprising a communication device, coupled to a physically separate network from the network that the data center is coupled to, to retrieve statistical data collected from network traffic flows collected by a plurality of monitors dispersed through the network that the data center is coupled to, with the monitors sending the statistical data collected from the network that the data center is coupled to over the physically separate network from the network that the plurality of monitors collect the statistical data from; analyzing the statistical data from the plurality of monitors and identifying malicious network traffic; and eliminate the malicious traffic from entering the data center.

Conclusion

Art Unit: 2136

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867.

The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

June 6, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


6, 7, 07